

Please add claims 2-82 as follows:

A¹
-2. A method for authenticating information about revoked certificates, comprising the steps

of:

- (a) storing the information about revoked certificates in an authentication tree; and
- (b) digitally signing the root value of the tree, wherein the root value contains less bits than a list of all revoked certificates.

3. A method according to claim 2, wherein the information about revoked certificates stored in the authentication tree includes the serial numbers of the revoked certificates.

4. A method according to claim 3, wherein the information about revoked certificates further includes revocation dates.

5. A method according to claim 2, wherein digitally signing is performed by a certification authority.

6. A method according to claim 4, wherein the information about revoked certificates is determined by a certification authority.

7. A method according to claim 4, wherein storing information is performed by a certification authority.

8. A method according to claim 2, wherein an entity that stores information also digitally signs the root.
9. A method according to claim 8, wherein the entity is a certification authority.
10. A method according to claim 8, wherein the entity is a directory.
11. A method according to claim 2, wherein a directory uses the authentication tree to prove that a certificate has been revoked.
12. A method according to claim 11, wherein the root is digitally signed by an entity other than the directory.
13. A method according to claim 12, wherein the root is digitally signed by a certification authority.
14. A method for authenticating information about valid certificates, comprising the steps of:
- (a) storing the information about valid certificates in an authentication tree; and
 - (b) digitally signing the root value of the tree, wherein the root value contains less bits than a list of all valid certificates.
15. A method according to claim 14, wherein the information about valid certificates stored in the authentication tree includes the serial numbers of the valid certificates.

- A1
cont
16. A method according to claim 14, wherein digitally signing is performed by a certification authority.
 17. A method according to claim 14, wherein the information about valid certificates is determined by a certification authority.
 18. A method according to claim 17, wherein storing information is performed by a certification authority.
 19. A method according to claim 14, wherein an entity that stores information also digitally signs the root.
 20. A method according to claim 19, wherein the entity is a certification authority.
 21. A method according to claim 19, wherein the entity is a directory.
 22. A method according to claim 14, wherein a directory uses the authentication tree to prove that a certificate is valid.
 23. A method according to claim 22, wherein the root is digitally signed by an entity other than the directory.

AI
conf

24. A method according to claim 23, wherein the root is digitally signed by a certification authority.

25. A method for authenticating information about valid and revoked certificates, comprising the steps of:

- (a) storing in an authentication tree information indicating whether each certificate is valid or revoked; and
- (b) digitally signing the root value of the tree, wherein the root value contains less bits than a list of all certificates.

26. A method according to claim 25, wherein the information includes the serial numbers of the certificates.

27. A method according to claim 26, wherein information about revoked certificates further includes revocation dates.

28. A method according to claim 25, wherein digitally signing is performed by a certification authority.

29. A method according to claim 28, wherein the information is determined by a certification authority.

- A¹
cont
30. A method according to claim 29, wherein storing information is performed by a certification authority.
 31. A method according to claim 25, wherein an entity that stores information also digitally signs the root.
 32. A method according to claim 31, wherein the entity is a certification authority.
 33. A method according to claim 31, wherein the entity is a directory.
 34. A method according to claim 25, wherein a directory uses the authentication tree to prove that a certificate has been revoked.
 35. A method according to claim 25, wherein a directory uses the authentication tree to prove that a certificate is valid.
 36. A method according to claim 34, wherein the root is digitally signed by an entity other than the directory.
 37. A method according to claim 36, wherein the root is digitally signed by a certification authority.

- AI
conf
38. A method according to claim 35, wherein the root is digitally signed by an entity other than the directory.
39. A method according to claim 38, wherein the root is digitally signed by a certification authority.
40. A method for providing authenticated information about a revoked certificate, comprising the steps of:
- (a) providing an information value stored in an authentication tree, wherein the information value contains information about the revoked certificate;
 - (b) providing an authenticated root value of the authentication tree; and
 - (c) providing an authentication path for the information value.
41. A method according to claim 40, wherein the information value includes the serial numbers of the revoked certificate.
42. A method according to claim 41, wherein the information value includes a revocation date.
43. A method according to claim 40, wherein the root value is authenticated by a digital signature.

- A!
cont
44. A method according to claim 43, wherein the digital signature is provided by a certification authority.
45. A method according to claim 43, wherein the digital signature is provided by a directory.
46. A method according to claim 40, wherein the information value is stored by a certification authority.
47. A method according to claim 40, wherein an entity that stores the information value also digitally signs the root of the authentication tree.
48. A method according to claim 47, wherein the entity is a certification authority.
49. A method according to claim 47, wherein the entity is a directory.
50. A method according to claim 40, wherein the authentication path is provided by a directory.
51. A method according to claim 50, wherein the directory stores the information value and authenticates the root value.

- A
Cont
52. A method according to claim 2, wherein the information about a particular revoked certificate is stored in a node of the authentication tree that depends upon the particular revoked certificate.
53. A method according to claim 13, wherein the information about a particular revoked certificate is stored in a node of the authentication tree that depends upon the particular revoked certificate.
54. A method according to claim 25, wherein the information about a particular revoked certificate is stored in a node of the authentication tree that depends upon the particular revoked certificate
55. A method according to claim 40, wherein the information about the revoked certificate is stored in a node of the authentication tree that depends upon the revoked certificate.
56. A method of providing information about revoked certificates, comprising the steps of:
- (a) storing, in nodes of a tree, information about the revoked certificates;
 - (b) for each internal node of the tree, obtaining a value that binds each internal node to values of the children thereof; and
 - (c) authenticating a root value of the tree.

- A1
cont
57. A method according to claim 56, wherein obtaining a value for a particular internal node includes evaluating a one-way function on at least values indicative of the children of the particular internal node.
58. A method according to claim 56, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.
59. A method according to claim 57, wherein a particular revoked certificate determines the path from the root of the tree to the node storing information about the particular revoked certificate.
60. A method according to claim 57, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.
61. A method according to claim 56, wherein a particular revoked certificate determines the path from the root of the tree to the node storing information about the particular revoked certificate.
62. A method according to claim 56, wherein the root value is digitally signed by a CA.
63. A method according to claim 56, wherein the root value is digitally signed by a directory.

64. A method according to claim 58, wherein the root value is digitally signed by a CA.

65. A method according to claim 59, wherein the root value is digitally signed by a CA.

66. A method according to claim 58, wherein the root value is digitally signed by a directory.

67. A method according to claim 59, wherein the root value is digitally signed by a directory.

68. A method according to claim 56, wherein information on at least two certificates is stored in the same node of the tree.

69. A method according to claim 58, wherein information on at least two certificates is stored in the same node of the tree.

70. A method according to claim 59, wherein information on at least two certificates is stored in the same node of the tree.

- A1
cont
71. A method of providing information about valid and revoked certificates, comprising the steps of:
- (a) storing, in nodes of a tree, information about certificates with an indication of whether the certificates are revoked;
 - (b) for each internal node of the tree, obtaining a value that binds each internal node to values of the children thereof; and
 - (c) authenticating a root value of the tree.
72. A method according to claim 71, wherein obtaining a value for a particular internal node includes evaluating a one-way function on at least values indicative of the children of the particular internal node.
73. A method according to claim 71, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.
74. A method according to claim 72, wherein a particular revoked certificate determines the path from the root of the tree to the node storing information about the particular revoked certificate.
75. A method according to claim 72, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.

- AI
cont
76. A method according to claim 71, wherein a particular revoked certificate determines the path from the root of the tree to the node storing information about the particular revoked certificate.
77. A method of providing information about valid certificates, comprising the steps of:
- (a) storing, in nodes of a tree, information about the valid certificates;
 - (b) for each internal node of the tree, obtaining a value that binds each internal node to values of the children thereof; and
 - (c) authenticating a root value of the tree.
78. A method according to claim 77, wherein obtaining a value for a particular internal node includes evaluating a one-way function on at least values indicative of the children of the particular internal node.
79. A method according to claim 77, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.
80. A method according to claim 77, wherein a particular revoked certificate determines the path from the root of the tree to the node storing information about the particular revoked certificate.
81. A method according to claim 78, wherein the node in which information about a particular revoked certificate is stored depends on the particular revoked certificate.